[19] Intellectual Property Bureau of the Peoples' Republic of China [51] Int. Cl[7]
E05B 49/00

[12] Invention Patent Public Announcement
[21] Application No.99804175.0

[43] Announcement Date: May 2, 2001 [11] Announcement No. CN 1293732A

[22] Date of Application: December 7, 1999 [21] Application No.: 99804175.0
[30] Priority Right:
[32] December 8, 1998 [33] US [31] 09/207,861
[86] International Application: PCT/US99/28933 December 7, 1999
[87] International Publication No.: WO00/34605 British June 15, 2000
[85] Date Entering National Phase: September 19, 2000
[71] Assignee: Microchip Technology, Inc.
Address: Arizona, USA
[72] Inventor: Y. LEE, P. SORRELLS, and A. C. KUZDAS

[74] Patent Representative Agency: Liu Shen Zhi Intellectual Property Attorney Law Office
Representative: MA Ying

Patent Claims 3 pages; Descriptions 7 pages; Graphs and Drawings 3 pages

[54] Name of Invention: A Radio Frequency Identification Security Device

[57] Abstract

An electronic key which is composed of a radio frequency identification (RFID) tag. Any time when the electronic key is not inserted into a lock, it short circuit or breaking conductor between RFID tag device and its resonant circuit or the antenna to block the RFID Input/Output (I/O). This is a security measure which prevents un-authorized personnel from reading the code of the electronic key through a secret/concealed reading device. As the electronic key is inserted into the electronic lock, the said circuit uses a matching short-circuit strip to close the contact point (normally open application) of the key, or uses a non-conductor spacer (separator) to open the short-circuited spring contact (normally closed application); forming a closed loop circuit. Once the circuit is forming a closed circuit, it initiates wireless data transmission from the electronic key to the electronic lock device.

(A simplified electrical schematic of the first application example of this invention is shown to the right)

Published by the Intellectual Publisher
ISSN 1008 – 4274

Patent Claims

1. A radio frequency identification (RFID) security device, which includes:

A key, in which the said key is consisting of:

A RFID tag device, used to store data in the said key;

a driver (excitation) circuit that is coupled to the RFID tag device mentioned, used to provide energy for the RFID tag mentioned for reading the data mentioned in the said key; and

a contact for the key that is coupled to the driver circuit mentioned, used to turn on or off the driving circuit mentioned.

2. A radio frequency identification (RFID) security device as in Claim 1, in which the said driver circuit is consisting of:

A resonance inductor; and

a resonance capacitor that is coupled to the resonance inductor mentioned.

3. A radio frequency identification (RFID) security device as in Claim 2, in which the resonance inductor mentioned is a coil.

4. A radio frequency identification (RFID) security device as in Claim 2, in which the resonance inductor mentioned is an antenna.

5. A radio frequency identification (RFID) security device as in Claim 2, in which the resonance inductor mentioned is located on the RFID tag device.

6. A radio frequency identification (RFID) security device as in Claim 1, in which the driver circuit mentioned is an antenna.

7. A radio frequency identification (RFID) security device as in Claim 1, in which the key contact mentioned is a normally open contact, such that when the key mentioned is inserted into the reading device, it turns off the driver circuit mentioned.

8. A radio frequency identification (RFID) security device as in Claim 7, in which the normally open key contact mentioned is located on the first outer side of the key mentioned.

9. A radio frequency identification (RFID) security device as in Claim 7, in which the normally open key contact mentioned is located on both the first and the second outer sides of the key mentioned, such that the insertion direction of the key mentioned is multi-directional (universal).

10. A radio frequency identification (RFID) security device as in Claim 1, in which the key contact mentioned is a normally closed contact, such that when the key mentioned is not inserted into the reading device, the driver circuit mentioned is shorted and is not functional.

11. A radio frequency identification (RFID) security device as in Claim 10, in which the normally closed contact mentioned is located on the inside of the key mentioned.

12. A radio frequency identification (RFID) security device as in Claim 10, in which the normally closed contact mentioned is located on the outside of the key mentioned.

13. A radio frequency identification (RFID) security device, which includes:

A electronic locking device; and

an electronic key, in which the said electronic key is consisting of:

A RFID tag device, used for storing data in the said electronic key;

when the electronic key mentioned and the electronic locking device are engaged, the driver circuit is electrically coupled to the RFID tag device mentioned; for providing energy to the RFID tag device mentioned to read the data mentioned on the electronic key, as the electronic key mentioned is engaged to the electronic device mentioned; and

the key contact coupled to the driving circuit is used to switch on the driver circuit mentioned when the electronic key mentioned is engaged to the electronic locking device mentioned.

14. A radio frequency identification (RFID) security device as in Claim 13, in which the said driver circuit is consisting of:

A resonance capacitor; and

a resonance inductor.

15. A radio frequency identification (RFID) security device as in Claim 14, in which the resonance inductor mentioned is located inside the electronic locking device mentioned, and when the electronic key mentioned is engaged to the electronic device mentioned, it is coupled to the resonance capacitor mentioned.

16. A radio frequency identification (RFID) security device as in Claim 14, in which both the resonance inductor and the resonance capacitor mentioned are located inside the electronic locking device mentioned, and when the electronic key mentioned is engaged to the electronic device mentioned, they are coupled to the RFID tag device mentioned.

17. A radio frequency identification (RFID) security device as in Claim 14, in which the resonance inductor mentioned is a coil.

18. A radio frequency identification (RFID) security device as in Claim 14, in which the resonance inductor mentioned is an antenna.

19. A radio frequency identification (RFID) security device as in Claim 14, in which the resonance inductor mentioned is located on the RFID tag device mentioned.

20. A radio frequency identification (RFID) security device as in Claim 13, in which the driver circuit mentioned is an antenna.

21. A radio frequency identification (RFID) security device as in Claim 13, in which the key contact mentioned is a normally open contact, such that when the key mentioned is not engaged to the electronic locking device, the driver circuit mentioned is disconnected.

22. A radio frequency identification (RFID) security device as in Claim 21, in which the normally open key contact mentioned is located on the first outer side of the electronic key mentioned.

23. A radio frequency identification (RFID) security device as in Claim 21, in which the normally open key contact mentioned is located on both the first and the second outer sides of the electronic key mentioned, such that the insertion direction of the electronic key mentioned is multi-directional (universal).

24. A radio frequency identification (RFID) security device as in Claim 13, in which the electronic locking device is including:

A reading device, used for reading the data transmitted from the electronic key mentioned when the electronic key and the electronic device mentioned are engaged; and

a first inductance element coupled to the reading device mentioned, used to transmit signal to the driver circuit of the electronic key mentioned, when the electronic key mentioned is engaged to the electronic locking device mentioned.

25. A radio frequency identification (RFID) security device as in Claim 24, in which the electronic locking device is also including:

A second inductance element that is coupled to the first inductance element mentioned; and

connecting components coupled to the second inductance element mentioned, for forming the driver circuit mentioned, when the second inductance element mentioned is engaged with the electronic key mentioned.

Descriptions

A Radio Frequency Identification Security Device

Background of Invention

Field of Invention

This invention is pertaining to a radio frequency identification (RFID) security device, especially concerning a RFID tag device that is forming an electronic key; when the key is not inserted into a locking device, where the electronic key is using a contact element, or through an antenna or a resonance inductor, to short or open the RFID tag device, blocking off the RFID I/O (input/output),.

Description of Current Technology

For a long time, electronic key has been used to prevent unauthorized entry to a restricted area. Recently, there are several types of electronic key are available in the market place. Although, different type of electronic keys is functioning to some extent, however, each has certain disadvantages.

One of such electronic keys is an electronic key based on an EEPROM (electrically erasable programmable read only memory) in series. To operate keys based on an EEPROM in series required 4 – 5 separate contacts. The contacts are used for power, ground, clock, and data, respectively. Two contacts may be used for data transmission (i.e., one for input contact, and the other for output contact). For keys based on an EEPROM in series each of the multiple contacts must maintain proper contact, for transmitting through clock and data information. When a key is used in an apartment or hotel, guest returning from a swimming pool may insert a wet key into a lock, which may cause poor contacts or shorts between contacts, so that data can not be properly transmitted, therefore, unable to open the lock. In addition, inserting the key with wrong polarity into the lock may also damage the electronic circuit or the EEPROM device, rendering the key useless. Therefore, moisture, insertion polarity, and wear and tear and/or damage of multiple contacts are the existing issues on this type of electronic key.

A second type of electronic key is using a RFID tag for access control. In this type of keys, a card or a tag is presented to a reading device to gain access to a building. In majority of cases, this type of key is used for identification rather than for security purpose. Since this type of key is not very secure, therefore, there is a concern when this type of electronic key is used for security purpose (for locks in an apartment and hotel). Concealed reader, even a battery operated reader, may apply power to the tag and steal its code without the knowledge of the user, even though the tag is still in the pocket or purse of a user.

One of the approaches to resolve the related security issue of the access control RFID tag is to use an encrypted electronic key. Several types of such electronic keys are available include algorithm encrypted chip (die). Certain algorithm encryption is allowing the code on the electronic key to be encrypted and changed every time the key is being read. Although these types of electronic keys may prevent unauthorized "code stealing", however, they are much more expensive than the RFID tag devices. For this reason, there is price for security.

Therefore, there is a need for providing an improved RFID security device. An improved RFID security device must not require several contact points for data transmission. An improved RFID security device must also be universal on polarity. An improved RFID security device must not be affected by environmental factors. And an improved RFID security device must also be able to be used for security purpose and is "code stealing" resistant. The improved RFID security device will use a RFID tag device to form an electronic key. Whenever a RFID security device is not inserted into the lock, the improved RFID security device will make the contact of the circuit between the RFID tag memory device and the antenna or resonance inductor to be shorted or open; thus prevent unauthorized persons from reading the key through a concealed reader.

Descriptions of Invention

According to one application example of this invention, one of the objectives of this invention is to provide an improved RFID security device.

Another objective of this invention is to provide an improved RFID security device which does not require several contact points for data transmission.

Another objective of this invention is also to provide an improved RFID security device which is universal in polarity.

Another objective of this invention is also to provide an improved RFID security device which is not affected by environmental factors.

Another objective of this invention is also to provide an improved RFID security device which can be used for security purpose and is an improved RFID security device and which is "code stealing" resistant.

Another objective of this invention is also to provide an improved RFID security device which is using a RFID tag device to form an electronic key.

Another objective of this invention is also to provide an improved RFID security device that any time when a RFID security device is not inserted into a lock, the improved RFID security device will make the contact of the circuit between the RFID tag memory device and the antenna or resonance inductor to be shorted or open; thus prevent unauthorized personnel from reading the key through a concealed reader.

Yet another objective of this invention is also to provide a device mentioned that is lower in cost comparing to an encrypted device.

Brief Descriptions of Preferred Application Examples

According to one application example of this invention, this invention discloses a radio frequency identification (RFID) security device. The radio frequency (RFID) security device is an electronic key. The electronic key uses a RFID tag device to store data on the key. A driver circuit is coupled to the RFID tag device and can provide energy to the RFID tag device and reading the data on the electronic key. The driver circuit may be a tuned resonance circuit or an antenna. Key contact is coupled to the driver circuit, and is used to turn on or off the driver circuit. Once the electronic key is activated, data can then be transmitted from the electronic key.

According to another application example of this invention, this invention discloses a radio frequency identification (RFID) security device. The RFID security device uses an electronic locking device and an electronic key. The electronic key has an RFID tag device that is used for storing data. When the electronic key and the electronic locking device are engaged, the driver circuit and the RFID tag device are coupled electrically. The driver circuit may be a tuned resonance circuit or an antenna. The driver circuit is used to provide energy to the RFID tag device, and to read the data from the electronic key when the electronic key and the electronic locking device are engaged. When the electronic key and the electronic locking device are engaged, the contact of the electronic key is coupled and connected to the driver circuit. When the electronic key and the electronic locking device are engaged, the electronic locking device is reading data transmitted from the electronic key through a reading device. When the electronic key and the electronic locking device are engaged, a first inductive element is coupled to the reading device, transmitting signal to the driver circuit of the electronic key. A second inductive element is coupled to the first inductive element. A circuit shorting component is coupled to the second inductive element, allowing the second inductive element to couple to the electronic key to form the driver circuit of the electronic key.

In conjunction with the attached figures, the preferred application examples of this invention are described below, so that the above mentioned and other objectives, characteristics, as well as advantages of this invention, will be even more clearly described.

Brief Descriptions of Attached Figures

Figure 1 is a simplified electrical schematic of the first application example of this invention.

Figure 2 is a simplified electrical schematic of the second application example of this invention.

Figure 3 is a simplified electrical schematic of the third application example of this invention.

Figure 4 is a simplified electrical schematic of the fourth application example of this invention.

Figure 5 is a simplified electrical schematic of the fifth application example of this invention.

Figure 6A is a top view of an implemented device of this invention.

Figure 6B is an end view of an application example of an implemented device of this invention described in 6A.

Figure 6C is an end view of a second application example of an implemented device of this invention described in 6A.

Figure 7A is a top view of another implemented device of this invention.

Figure 7B is an end view of an application example of an implemented device of this invention described in 7A.

Figure 7C is an end view of a second application example of an implemented device of this invention described in 7A.

Figure 8A is a top view of yet another implemented device of this invention.

Figure 8B is a side view of an implemented device described in 8A.

Figure 8C is an end view of an implemented device described in 8A.

Figure 9 is a simplified electrical schematic of yet another application example of this invention.

Detailed Descriptions of Preferred Application Examples

Referring to Figure 1, which is depicting an improved electronic key 10 (referred to as key 10 below) of the First Application Example. The key 10 is using a radio frequency identification (RFID) tag device 12. The RFID tag device is programmed to store data in key 10. When the key 10 is inserted into a locking device (not shown), the reading device (not shown) in the locking device is reading the data stored in the RFID tag device 12. If a proper electronic key 10 is inserted into the locking device, then the locking device will be released.

In order to read the data in the RFID tag device 12, the driver circuit 14 is engaged to the RFID tag device 12. The driver circuit 14 is used to provide energy to the RFID tag device 12, and to transmit data signal back to the reader. The driver circuit may be a tuned resonance circuit or an antenna. In the application example depicted in Figure 1, the driver circuit 14 is a tuned resonance circuit 14. The reading device of the locking device sends out a carrier signal. The tuned resonance circuit 14 is using the energy from the carrier signal to provide electrical power to the RFID tag device 12; which allows the reading device of the locking device to read the data stored in the RFID tag device. The tuned resonance circuit 14 includes an inductance element 16 and a capacitor element 18. The inductance element 16 may be any kind of inductor, for example, an antenna or a coil.

Contact device 20 and tuned resonance circuit 14 are coupled. Contact device 20 is used to connect or disconnect tuned resonance circuit 14. In the application example depicted in Figure 1, contact device 20 is a normally open contact. When the key 10 is inserted into the electronic locking device, the shorting strip in the locking device closes contact device 20, thus forming a closed tuned resonance circuit 14. Once the tuned resonance circuit 14 becomes a closed circuit, it initiates the supply of power to the RFID tag device 12 and transmission of data from the key 10 to the electronic locking device.

Referring to Figure 2, which is depicting a second application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application example depicted in Figure 1. The main difference is that contact circuit 20 is used to establish an open circuit between the entire tuned resonance circuit 14 and RFID tag device 12. In the application example depicted in Figure 2, the contact device 20 is a normally open contact. When the key 10 is inserted into the electronic locking device, the shorting strip in the locking device closes contact device 20, thus forming a closed tuned resonance circuit 14. Once the tuned resonance circuit 14 becomes a closed circuit, it initiates the supply of power to the RFID tag device 12 and transmission of data from the key 10 to the electronic locking device.

Referring to Figure 3, which is depicting a third application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application examples depicted in Figures 1 and 2. The main difference is that a capacitor element 18 is located on the RFID tag device. The key 10 in Figure 3 serves similar function as the key 10's depicted in Figures 1 and 2. In the application example depicted in Figure 3, the contact device 20 is a normally open contact. When the key 10 is inserted into the electronic locking device, the shorting strip in the locking device closes contact device 20, thus forming a closed tuned resonance circuit 14. Once the tuned resonance circuit 14 becomes a closed circuit, it initiates the supply of power to the RFID tag device 12 and

transmission of data from the key 10 to the electronic locking device.

Referring to Figure 4, which is depicting a fourth application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application example depicted in Figure 3. The main difference is that in the driver circuit 14, the inductive element 16 is an antenna. In the preferred application examples of this invention, the antenna is a microwave antenna. The key 10 in Figure 4 is functioning in a similar fashion as the key 10's depicted in Figures 1 – 3.

Referring to Figure 5, which is depicting a fifth application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application example depicted in Figure 4. The main difference is that the contact device 20 is a normally closed contact device. The normally closed contact device 20 will establish a short circuit between the terminals of the driver circuit 14, thus breaking off the key 10. In this application example, when the key 10 is inserted into the electronic locking device (not shown), a non-conductor spacer forces the shorted contact device 20 to open, thus turn on the driver circuit 14. Once the driver circuit 14 is turn on, it initiates the supply of power to the RFID tag device 12 and transmission of data from the key 10 to the electronic locking device. It should be noted that in the application example depicted in Figure 5, a tuned inductor is used to replace the antenna. The tuned inductor is functioning in a similar fashion as depicted in Figures 1 – 3.

Referring to Figure 6A, which is depicting a sixth application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application examples depicted in Figures 3 and 4 in which capacitor elements are mounted on the RFID tag device; and very similar to the application examples depicted in Figures 1 and 2 in which the capacitor elements 18 are mounted on an external module relative to RFID tag device 12. In the application example depicted in Figure 6A, contact devices 20 are a pair of normally open contact elements; the pair of contact elements may be on one or more sides of the key 10. In addition, as can be seen in Figure 6B, contact devices 20 are extended (protruded) from the key 10; or may be as shown in Figure 6C, where contact devices 20 are embedded in the key 10 allowing the contact elements to be flush with the key 10. When the key 10 is inserted into the electronic device, shorting strips in the electronic device close contact devices 20, thus forming a closed driver circuit 14. Driver circuit 14 may be a tuned resonance circuit or an antenna. Once the tuned resonance inductor circuit 14 is forming a closed circuit or is in the alternative (alternating current ?) status, the RFID tag device is coupled to the antenna, initiating data transmission from the key 10 to the electronic locking device.

Referring to Figure 7A, which is depicting a seventh application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application examples depicted in Figures 6A – 6C. In the application example depicted in Figure 7A, contact devices 20 are also a pair of normally open contact elements. However, in this application example, one of the contact elements is located on one side of the key 10, while the other contact element is on the other side of the key 10. As in the previous application example, as can be seen in Figure 7B, contact devices 20 are extended from the key 10; or may be as shown in Figure 7C, where contact devices 20 are embedded in the key 10 allowing the contact elements to be flush with the key 10. As in the previous application example, when the key 10 is inserted into the electronic device, shorting

strips in the electronic device close contact devices 20 forming a closed driver circuit 14. Driver circuit 14 may be a tuned resonance circuit or an antenna. Once the tuned resonance inductor circuit 14 is forming a closed circuit or is in the alternative (alternating current ?) status, the RFID tag device is coupled to the antenna, initiating data transmission from the key 10 to the electronic locking device.

Referring to Figure 8A, which is depicting an eighth application example of the key 10; in which similar numbers and symbols are used to represent the same elements. The application example is very similar to the application examples depicted in Figures 7A – 7C. In the application example depicted in Figure 8A, the primary difference is that the contact devices 20 are a pair of normally closed contact elements 22. The normally closed contact elements 22 usually are a pair of normally closed spring contact elements. In this application example, the key 10 is hollow. When the key 10 is inserted into the electronic locking device, a non-conductor spacer will be inserted into the hollow key 10. The non-conductor spacer is making the pair of normally closed contact device 22 open, thus connecting the driver circuit 14. Once the tuned resonance inductor circuit 14 is forming a closed circuit or is not being shorted, data transmission from the key 10 to the electronic locking device is being initiated.

Now, referring to Figure 9, which is depicting yet another application example of this invention, in which similar numbers and symbols are used to represent the same elements. In this application example which is showing a RFID security system 30 (referred to as the system 30 below). The system 30 is using an electronic key 10 and an electronic locking device 40. In this application example, the electronic key 10 has a RFID tag device 12 which is programmed to store data in the key 10. The RFID tag device may also further contain a capacitor element 18 located on the device. However, the capacitor element 18 may be located on the die, module, or may not even be needed if an antenna is used. The contact device 20 is coupled to the RFID tag device 10. In the application example depicted in Figure 9, the contact device 20 is a normally open contact. In this application example, the contact devices 20 use a pair of contact elements. One contact element is located on one side of the key 10, while the other contact element is located on the other side of the key 10. As the application examples described in Figures 7A – 7C, the contact devices 20 may be extended from the key 10 as can be seen in Figure 7B; or may be as shown in Figure 7C, the contact devices 20 are embedded in the key 10, allowing the contact elements to be flush with the key 10.

The electronic locking device 40 is using a reading device 42 to read the data stored in the RFID tag device 12 of the key 10. The reading device 42 is coupled to the inductive element 44.

The reading device 42 is sending out carrier signal through an inductive element 44. The driver circuit 14 of the electronic key 10, located inside the electronic locking device, receives the said carrier signal. The driver circuit 14 provides power to the RFID tag device 12, using the energy from the carrier signal; which allows the reading device 42 of the electronic locking device 40 to read the data stored in the RFID tag device.

In the application example described in Figure 9, the electronic locking device 40 also has a second inductive element 16. Similar to the previous application example, the second inductive element 16 is combined with the capacitor element 18 to form a driver circuit 14. A connecting element 46 is coupled to the second inductive element 16. When the key 10 is inserted into the electronic device 40, the connecting element 46 in the electronic device 40 is connecting to the contact device 20, thus allowing the driver circuit 14 to form a closed circuit. Once the tuned resonance inductor circuit 14 is forming a closed

circuit, it provides power to the RFID tag device 12 using the energy from the carrier signal transmitted from the inductive element 44; which initiates data transmission from the key 10 to the electronic locking device; thus allowing the reading device 42 of the locking device 40 to read the data stored in the RFID tag device 12.

Although the invention has been described with specific figures through the preferred application examples of this invention, technical persons who are in the field should understand that various changes in forms and details may be made without departing from the spirit and scope of this invention.

Attached Figures

(Figures 1 through 9, as described in earlier section, are attached).

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
E05B 49/00

[12]发明专利申请公开说明书

[21]申请号 99804175.0

[43]公开日 2001年5月2日

[11]公开号 CN 1293732A

[22]申请日 1999.12.7 [21]申请号 99804175.0
[30]优先权
[32]1998.12.8 [33]US [31]09/207,861
[86]国际申请 PCT/US99/28933 1999.12.7
[87]国际公布 WO00/34605 英 2000.6.15
[85]进入国家阶段日期 2000.9.19
[71]申请人 密克罗奇普技术公司
地址 美国亚利桑那州
[72]发明人 尤博克·李 彼得·察留尔斯
阿德里安·C·库兹达斯

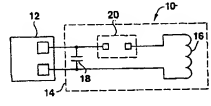
[74]专利代理机构 柳沈知识产权律师事务所
代理人 马 莹

权利要求书3页 说明书7页 附图页数3页

[54]发明名称 射频识别安全装置

[57]摘要

一种电子钥匙由射频识别(RFID)标签装置构成。电子钥匙通过在未插入锁中的任何时候短路或断开RFID标签装置与它的谐振电路或天线之间的导体来阻断RFID输入/输出(I/O)。这是防止非法人员通过秘密/隐藏的阅读装置读取电子钥匙代码的安全措施。该电路是通过当电子钥匙插入电子锁装置时,利用匹配短路条闭合钥匙触点(常开应用),或利用非导体隔离板张开短路的弹簧触点(常闭应用)。形成闭合回路的。一旦电路形成闭合回路,就启动数据从电子钥匙到电子锁装置的无线传送。



ISSN1008-4274

权 利 要 求 书

1. 一种射频识别(RFID)安全装置，包括：

一个钥匙，其中所述钥匙包括：

RFID 标签装置，用于将数据存储在所述钥匙上；

与所述 RFID 标签装置耦合的激励电路，用于将能量提供给所述 RFID 标签装置以读取在所述钥匙上的所述数据；和

与所述激励电路耦合的钥匙触点，用于接通和断开所述激励电路。

2. 根据权利要求 1 所述的射频识别(RFID)安全装置，其中所述激励电路包括：

谐振电感器；和

与所述谐振电感器耦合的谐振电容器。

3. 根据权利要求 2 所述的射频识别(RFID)安全装置，其中所述谐振电感器是线圈。

4. 根据权利要求 2 所述的射频识别(RFID)安全装置，其中所述谐振电感器是天线。

5. 根据权利要求 2 所述的射频识别(RFID)安全装置，其中所述谐振电容器位于所述 RFID 标签装置上。

6. 根据权利要求 1 所述的射频识别(RFID)安全装置，其中所述激励电路是天线。

7. 根据权利要求 1 所述的射频识别(RFID)安全装置，其中所述钥匙触点是常开触点，以便当所述钥匙未插入用于阅读的装置中时断开所述激励电路。

8. 根据权利要求 7 所述的射频识别(RFID)安全装置，其中所述常开触点位于所述钥匙的第一外侧上。

9. 根据权利要求 7 所述的射频识别(RFID)安全装置，其中所述常开触点位于所述钥匙的第一外侧和第二外侧上，以便使所述钥匙的插入方向是多向的(universality)。

10. 根据权利要求 1 所述的射频识别(RFID)安全装置，其中所述钥匙触点是常闭触点，以便当所述钥匙未插入用于阅读的装置中时短路所述激励电路使其不起作用。

11. 根据权利要求 10 所述的射频识别(RFID)安全装置，其中所述常闭触点位于所述钥匙的内部。

12. 根据权利要求 10 所述的射频识别(RFID)安全装置，其中所述常闭触点位于所述钥匙的外部。

13. 一种射频识别(RFID)安全装置，包括：

电子锁装置；和

电子钥匙，其中所述电子钥匙包括：

RFID 标签装置，用于将数据存储在所述电子钥匙上；

当所述电子钥匙与所述电子锁装置耦合时与所述 RFID 标签装置电耦合的激励电路，用于当所述电子钥匙与所述电子锁装置耦合时将能量提供给所述 RFID 标签装置以读取在所述电子钥匙上的所述数据；和

与所述激励电路耦合的钥匙触点，用于当所述电子钥匙与所述电子锁装置耦合时接通所述激励电路。

14. 根据权利要求 13 所述的射频识别(RFID)安全装置，其中所述激励电路包括：

谐振电容器；和

谐振电感器。

15. 根据权利要求 14 所述的射频识别(RFID)安全装置，其中所述谐振电感器位于所述电子锁装置中，并且当所述电子钥匙与所述电子锁装置耦合时与所述谐振电容器耦合。

16. 根据权利要求 14 所述的射频识别(RFID)安全装置，其中所述谐振电感器和谐振电容器都位于所述电子锁装置中，并且当所述电子钥匙与所述电子锁装置耦合时与所述 RFID 标签装置耦合。

17. 根据权利要求 14 所述的射频识别(RFID)安全装置，其中所述谐振电感器是线圈。

18. 根据权利要求 14 所述的射频识别(RFID)安全装置，其中所述谐振电感器是天线。

19. 根据权利要求 14 所述的射频识别(RFID)安全装置，其中所述谐振电容器位于所述 RFID 标签装置上。

20. 根据权利要求 13 所述的射频识别(RFID)安全装置，其中所述激励电路是天线。

21. 根据权利要求 13 所述的射频识别(RFID)安全装置，其中所述钥匙触点是常开触点，以便当所述电子钥匙未与所述电子锁装置耦合时断开所述激励电路。

22. 根据权利要求 21 所述的射频识别(RFID)安全装置，其中所述常开触点位于所述电子钥匙的第一外侧上。

23. 根据权利要求 21 所述的射频识别(RFID)安全装置，其中所述常开触点位于所述电子钥匙的第一外侧和第二外侧上，以便使所述电子钥匙插入所述电子锁装置的方向是多向的。

24. 根据权利要求 13 所述的射频识别(RFID)安全装置，其中所述电子锁装置包括：

阅读装置，用于当所述电子钥匙与所述电子锁装置耦合时读取从所述电子钥匙传送的数据；和

与所述阅读装置耦合的第一电感单元，用于当所述电子钥匙与所述电子锁装置耦合时将信号传送到所述电子钥匙的所述激励电路。

25. 根据权利要求 24 所述的射频识别(RFID)安全装置，其中所述电子锁装置还包括：

与所述第一电感单元磁耦合的第二电感单元；和

与所述第二电感单元耦合的连接部件，用于使所述第二电感单元与所述电子钥匙相耦合以形成所述激励电路。

说　明　书

射频识别安全装置

发明背景

发明领域

本发明一般涉及射频识别(RFID)安全装置，尤其涉及构成电子钥匙的RFID标签装置，当钥匙未插入锁装置时，所述电子钥匙利用触点单元从天线或谐振电感器短路或断开RFID标签装置来阻断RFID I/O(输入/输出)。

现有技术描述

长期以来，电子钥匙已经被用于防止非法进入禁区。最近，市场上有几种不同类型的电子钥匙。虽然各种类型的钥匙的确起到一些作用，但它们的每一种都存在着某些缺陷。

一种这种类型的电子钥匙是基于串行EEPROM(电可擦可编程只读存储器)的电子钥匙。为了进行操作，串行EEPROM钥匙需要4-5个分开的触点。每个触点用于电源、地、时钟和数据的每一个。两个触点可以用于数据传输(即，一个作为输入触点，另一个作为输出触点)。在串行EEPROM钥匙中多个触点的每一个必须保持适当的接触，以便传输通过它们的时钟和数据。在公寓或旅馆应用中，从游泳池返回的旅客可能将湿的钥匙插入到锁中。这会使接触不好或使触点之间短路，数据得不到正确传输，从而使锁无法打开。此外，以错误极性将钥匙插入到锁中也将使锁电子线路或EEPROM装置损坏，从而使钥匙失去作用。因此，潮湿、插入极性、以及对多个接点的磨损和/或损坏都是这种类型的电子钥匙所存在的问题。

第二种类型的电子钥匙利用了入口控制FRID标签。在这些类型的钥匙中，向读取装置出示一张片卡或标签，以获准进入建筑物的入口。在大多数情况下，这种类型的电子钥匙用于识别用途而不是用于安全。由于这些类型的钥匙并非十分安全，因此，将这种类型电子钥匙用于安全(公寓和旅馆的锁)会引起问题。隐蔽的阅读器，甚至电池式阅读器，都能对标签加电并在没有用户资料的情况下窃取其代码，那怕标签在用户的衣袋或钱包中。

解决与入口控制RFID标签有关的问题的一种途径是拥有加密的电子钥匙。几种这种类型的电子钥匙包括在模(die)本身上的加密算法。一些加密算

法使电子钥匙上的代码每当钥匙被阅读时得到加密和改变。虽然这些类型的电子钥匙防止了非法“代码窃取”，但它们要比 RFID 标签装置昂贵得多。因此，安全是以金钱为代价的。

于是，存在着提供改进型 RFID 安全装置的需要。改进型 RFID 安全装置必须不需要若干个触点用于数据传输。改进型 RFID 安全装置还必须在极性上是通用的。改进型 RFID 安全装置必须不受环境因素影响。改进型 RFID 安全装置还必须能够用于安全需要和防“代码窃取”的。改进型 RFID 安全装置将利用构成电子钥匙的 RFID 标签装置。改进型 RFID 安全装置将利用在 RFID 安全装置未插入锁中的任何时候短路或断开 RFID 标签存储器装置与天线或谐振电感器之间的电路的触点，从而防止非法人员通过隐藏的阅读器阅读钥匙。

发明概述

根据本发明的一个实施例，本发明的一个目的是提供一种改进型 RFID 安全装置。

本发明的另一个目的是提供一种不需要若干个触点进行数据传输的改进型 RFID 安全装置。

本发明还有一个目的是提供一种在极性上通用的改进型 RFID 安全装置。

本发明还有一个目的是提供一种不受环境因素影响的改进型 RFID 安全装置。

本发明还有一个目的是提供一种能够用于安全需要并且还必须防“代码窃取”的改进型 RFID 安全装置。

本发明还有一个目的是提供一种利用构成电子钥匙的 RFID 标签装置的改进型 RFID 安全装置。

本发明还有一个目的是提供一种利用在 RFID 安全装置未插入锁中的任何时候短路或断开 RFID 标签存储器装置与天线或谐振电感器之间的电路的触点，从而防止非法人员通过隐藏的阅读器阅读钥匙的改进型 RFID 安全装置。

本发明再有一个目的是提供与加密装置相比成本降低了的上述装置。

优选实施例简述

根据本发明的一个实施例，本发明公开了一种射频识别(RFID)安全装

置。这种 RFID 安全装置是电子钥匙。这种电子钥匙利用 RFID 标签装置将数据存储在钥匙上。激励电路与 RFID 标签装置耦合将能量提供给 RFID 标签装置并读取电子钥匙上的数据。激励电路可以是调谐谐振电路或天线。钥匙触点与激励电路耦合。钥匙触点用于接通和断开激励电路。一旦电子钥匙起作用，就可能发生数据从电子钥匙传输出来。

根据本发明的另一个实施例，本发明公开了一种射频识别(RFID)安全装置。这种 RFID 安全装置使用电子锁装置和电子钥匙。电子钥匙拥有用于存储数据的 RFID 标签装置。当电子钥匙与电子锁装置耦合时，激励电路与 RFID 标签装置电耦合。激励电路可以是调谐谐振电路或天线。激励电路用于将能量提供给 RFID 标签装置，以便当电子钥匙与电子锁装置耦合时读取电子钥匙上的数据。当电子钥匙与电子锁装置耦合时钥匙触点与激励电路耦合接通激励电路。当电子钥匙与电子锁装置耦合时电子锁装置利用阅读装置阅读从电子钥匙传输的数据。当电子钥匙与电子锁装置耦合时，第一电感单元与阅读装置耦合，将信号传输到电子钥匙的激励电路。第二电感单元与第一电感单元耦合。短路部件与第二电感单元耦合，以便使第二电感单元与电子钥匙耦合形成电子钥匙的激励电路。

通过结合附图对本发明的优选实施例进行如下详细描述，本发明的上述和其它目的、特征和优点将更加清楚。

附图简述

图 1 是本发明第一实施例的简化电路示意图；

图 2 是本发明第二实施例的简化电路示意图；

图 3 是本发明第三实施例的简化电路示意图；

图 4 是本发明第四实施例的简化电路示意图；

图 5 是本发明第五实施例的简化电路示意图；

图 6A 是本发明一种实施装置的俯视图；

图 6B 是图 6A 所描绘的实施装置的一个实施例的端视图；

图 6C 是图 6A 所描绘的实施装置的第二个实施例的端视图；

图 7A 是本发明另一种实施装置的俯视图；

图 7B 是图 7A 所描绘的实施装置的一个实施例的端视图；

图 7C 是图 7A 所描绘的实施装置的第二个实施例的端视图；

图 8A 是本发明再一种实施装置的俯视图；

图 8B 是图 8A 所描绘的实施装置的侧视图；

图 8C 是图 8A 所描绘的实施装置的端视图；

图 9 是本发明再一个实施例的简化电路示意图。

优选实施例详述

参照图 1，图 1 显示了改进型电子钥匙 10(下文称为钥匙 10)的第一实施例。钥匙 10 利用射频识别(RFID)标签装置 12。对 RFID 标签装置 12 进行编程使数据存储在钥匙 10 上。当钥匙 10 插入锁装置(图中未示出)中时，存储在 RFID 标签装置 12 上的数据将由锁装置中的阅读装置(图中未示出)读取。如果已经将合适的电子钥匙 10 插入到锁装置中，那么，锁装置就会释放。

为了读取 RFID 标签装置 12 上的数据，将激励电路 14 与 RFID 标签装置 12 耦合。激励电路 14 用于将能量提供给 RFID 标签装置 12 并将数据信号传送回到阅读器。激励装置可以是调谐谐振电路或天线。在图 1 所描绘的实施例中，激励电路 14 是调谐谐振电路 14。锁装置的阅读装置发送出载波信号。将调谐谐振电路 14 调谐到载波信号的频率上。调谐谐振电路 14 将利用来自载波信号的能量向 RFID 标签装置 12 供电。这将使锁装置的阅读装置读取存储在 RFID 标签装置 12 上的数据。调谐谐振电路 14 包括电感单元 16 和电容单元 18。电感单元 16 可以是任何类型的电感器，例如，天线或线圈。

触点装置 20 与调谐谐振电路 14 耦合。触点装置 20 用于接通和断开调谐谐振电路 14。在图 1 所描绘的实施例中，触点装置 20 是常开触点。当钥匙 10 插入电子锁装置时，电子锁装置中的短路条将闭合触点装置 20，从而形成闭合的调谐谐振电路 14。一旦调谐谐振电路 14 形成闭合回路，就启动了向 RFID 标签装置 12 的供电和数据从钥匙 10 到电子锁装置的传送。

参照图 2，图 2 显示了钥匙 10 的第二实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 1 所描绘的实施例非常类似。主要差异在于，触点电路 20 用于建立整个调谐谐振电路 14 与 RFID 标签装置 12 之间的开路。图 2 中的钥匙 10 以与图 1 所示的钥匙 10 相同的方式起作用。在图 2 所描绘的实施例中，触点装置 20 是常开触点。当钥匙 10 插入电子锁装置时，电子锁装置中的短路条将闭合触点装置 20，从而形成闭合的调谐谐振电路 14。一旦调谐谐振电路 14 形成闭合回路，就启动了向 RFID 标签装置 12 的供电和数据从钥匙 10 到电子锁装置的传送。

参照图 3，图 3 显示了钥匙 10 的第三实施例，其中相同的标号和符号表

示相同的单元。这个实施例与图 1 和 2 所描绘的实施例非常类似。主要差异在于，电容单元 18 位于 RFID 标签装置 12 上。图 3 中的钥匙 10 以与图 1 和 2 所示的钥匙 10 相同的方式起作用。在图 3 所描述的实施例中，触点装置 20 是常开触点。当钥匙 10 插入电子锁装置时，电子锁装置中的短路条将闭合触点装置 20，从而形成闭合的调谐谐振电路 14。一旦调谐谐振电路 14 形成闭合回路，就启动了向 RFID 标签装置 12 的供电和数据从钥匙 10 到电子锁装置的传送。

参照图 4，图 4 显示了钥匙 10 的第四实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 3 所描绘的实施例非常类似。主要差异在于，在激励电路 14 中，电感单元 16 是一个天线。在本发明的优选实施例中，天线是微波天线。图 4 中的钥匙 10 以与图 1-3 所示的钥匙 10 相同的方式起作用。

参照图 5，图 5 显示了钥匙 10 的第五实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 4 所描绘的实施例非常类似。主要差异在于，触点装置 20 是常闭触点装置。常闭触点装置 20 将在激励电路 14 的端点之间建立起短路，从而断开钥匙 10。在本实施例中，当钥匙 10 插入电子锁装置(图中未示出)时，非导体隔离片使短路触点装置 20 张开，从而接通激励电路 14。一旦接通激励电路 14，就启动了向 RFID 标签装置 12 的供电和数据从钥匙 10 到电子锁装置的传送。应该注意到，在图 5 所描绘的实施例中，调谐电感器可以用来取代天线。调谐电感器以与图 1-3 所描述的相同方式起作用。

参照图 6A，图 6A 显示了钥匙 10 的第六实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 3 和 4 所描绘的其中电容单元安装在 RFID 标签装置 12 上的实施例非常类似，并与图 1 和 2 所描绘的其中电容单元 18 安装在相对于 RFID 标签装置 12 来说是外部的模块上的实施例类似。在图 6A 所描述的实施例中，触点装置 20 利用一对常开触点单元。这对触点单元可以在钥匙 10 的一边或多边上。此外，正如可以从图 6B 所看到的，触点装置 20 可以从钥匙 10 伸出来，也可以如从图 6C 所看到的，触点装置 20 可以嵌入钥匙 10 中以便使触点单元与钥匙 10 齐平。当钥匙 10 插入电子锁装置时，电子锁装置中的短路条将闭合触点装置 20，从而形成闭合的激励电路 14。激励电路 14 可以是调谐谐振电路或天线。一旦调谐谐振电路 14 形成

闭合回路或处于交流状态，RFID 标签装置 12 就与天线耦合，启动数据从钥匙 10 到电子锁装置的传送。

参照图 7A，图 7A 显示了钥匙 10 的第七实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 6A-6C 所描绘的实施例非常类似。在图 7A 所描述的实施例中，触点装置 20 也利用一对常开触点单元。然而，在此实施例中，一个触点单元位于钥匙 10 的一边，另一个触点单元位于钥匙 10 的另一边。如图前面的实施例一样，触点装置 20 可以从钥匙 10 伸出来，如图 7B 所示，或者，正如可以如从图 7C 看到的，触点装置 20 可以嵌入钥匙 10 中以便使触点单元与钥匙 10 齐平。与前面的实施例一样，当钥匙 10 插入电子锁装置时，电子锁装置中的短路条将闭合触点装置 20，从而形成闭合的激励电路 14。激励电路 14 可以是调谐谐振电路或天线。一旦调谐谐振电路 14 形成闭合回路或处于交流(alternative)状态，RFID 标签装置 12 就与天线耦合，启动数据从钥匙 10 到电子锁装置的传送。

参照图 8A，图 8A 显示了钥匙 10 的第八实施例，其中相同的标号和符号表示相同的单元。这个实施例与图 7A-7C 所描绘的实施例非常类似。在图 8A 所描绘的实施例中主要差异在于，触点装置 20 使用了一对常闭触点单元 22。常闭触点单元 22 通常是一对常闭弹簧触点单元。在此实施例中，钥匙 10 是中空的。当钥匙 10 插入电子锁装置时，非导体隔离片将插入空心钥匙 10 中。非导体隔离片使这对常闭触点装置 22 张开，从而接通激励电路 14。激励电路 14 可以是调谐谐振电路或天线。一旦调谐谐振电路 14 形成闭合回路，或未被短路，就启动数据从钥匙 10 到电子锁装置的传送。

现在参照图 9，图 9 显示了本发明的再一个实施例，其中相同的标号和符号表示相同的单元。在这个实施例中，显示了 RFID 安全系统 30(下文称为系统 30)。系统 30 利用了电子钥匙 10 和电子锁装置 40。在此实施例中，电子钥匙 10 拥有可以被编程成将数据存储在钥匙 10 上的 RFID 标签装置 12。RFID 标签装置 12 还可以含有位于其中的电容单元 18。然而，电容单元 18 可以位于模上、模块上、或者如果使用了天线的话甚至可以不需要。触点装置 20 与 RFID 标签装置 10 耦合。在图 9 所描绘的实施例中，触点装置 20 是常开触点。在此实施例中，触点装置 20 使用了一对触点单元。一个触点单元位于钥匙 10 的一边，而另一个触点单元则位于钥匙 10 的另一边。如同图 7A-7C 所描绘的实施例一样，触点装置 20 可以从钥匙 10 伸出，如图 7B 所

示，或者，正如可以从图 7C 看到的，触点装置 20 也可以嵌入钥匙 10 中使触点单元与钥匙 10 齐平。

电子锁装置 40 利用阅读装置 42 读取存储在钥匙 10 的 RFID 标签装置 12 上的数据。阅读装置 42 与电感单元 44 耦合。

阅读装置 42 将通过电感单元 44 发送载波信号。位于电子锁装置内部的、电子钥匙 10 的激励电路 14 接收该载波信号。激励电路 14 将采用来自载波信号的能量并对 RFID 标签装置 12 供电。这将使电子锁装置 40 的阅读装置 42 读取存储在 RFID 标签装置 12 中的数据。

在图 9 所描绘的实施例中，电子锁装置 40 还拥有第二电感单元 16。与前面实施例中的一样，第二电感单元 16 与电容单元 18 组合在一起形成激励电路 14。连接单元 46 与第二电感单元 16 相耦合。当钥匙 10 插入电子锁装置 40 时，电子锁装置 40 中的连接单元 46 将与触点装置 20 相连接，从而使激励电路 14 形成闭合回路。一旦激励电路 14 形成闭合回路，它就采用来自从电感单元 44 发送的载波信号的能量向 RFID 标签装置 12 供电。启动了数据从钥匙 10 到电子锁装置 40 的传送，从而使电子锁装置 40 的阅读装置 42 读取存储在 RFID 标签装置 12 中的数据。

虽然通过参照本发明的优选实施例对本发明进行了具体图示和描述，但本领域的技术人员应该明白，可以对其进行形式上和细节上的各种改动，而均不偏离本发明的精神和范围。

说 明 书 附 图

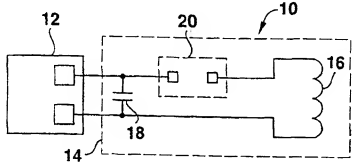


图 1

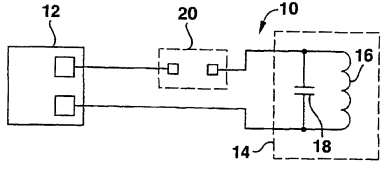


图 2

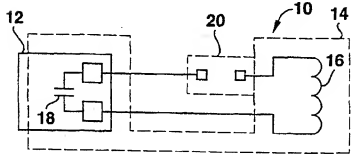


图 3

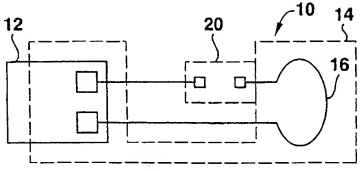


图 4

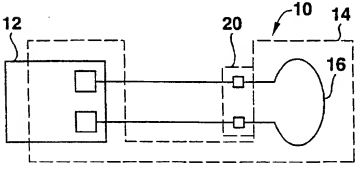


图 5

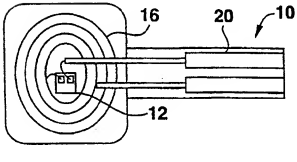


图 6A

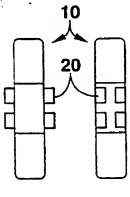


图 6B 图 6C

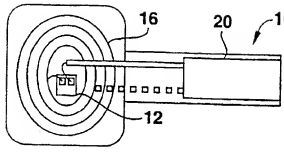


图 7A

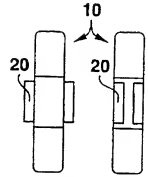


图 7B

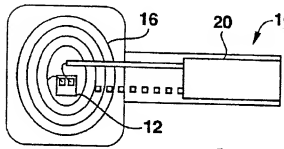


图 8A

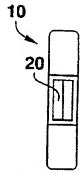


图 8C

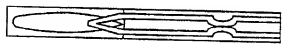


图 8B

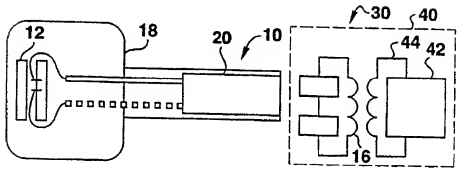


图 9